



US009047493B1

(12) **United States Patent**
Izhar

(10) **Patent No.:** **US 9,047,493 B1**
(45) **Date of Patent:** **Jun. 2, 2015**

(54) **SYSTEM AND METHOD FOR PROTECTING CONTENT**

(56) **References Cited**

U.S. PATENT DOCUMENTS

(75) Inventor: **Amnon Izhar**, Brookline, MA (US)
(73) Assignee: **EMC Corporation**, Hopkinton, MA (US)
(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 299 days.

5,748,744 A *	5/1998	Levy et al.	380/52
6,944,769 B1 *	9/2005	Daniels et al.	713/188
8,601,169 B1 *	12/2013	Paragaonkar et al.	710/6
2001/0025340 A1	9/2001	Marchant	
2005/0123139 A1 *	6/2005	Chin	380/265
2006/0069870 A1	3/2006	Nicholson et al.	
2009/0193184 A1	7/2009	Yu et al.	
2009/0210611 A1	8/2009	Mizushima	
2010/0031062 A1 *	2/2010	Nishihara et al.	713/193
2011/0289261 A1	11/2011	Candelaria	

* cited by examiner

Primary Examiner — Jung Kim

Assistant Examiner — Tri Tran

(74) *Attorney, Agent, or Firm* — Brian J. Colandreo; Mark H. Whittenberger; Holland & Knight LLP

(21) Appl. No.: **13/539,404**

(22) Filed: **Jun. 30, 2012**

(51) **Int. Cl.**
G06F 21/78 (2013.01)
H04L 29/08 (2006.01)
G06F 3/06 (2006.01)

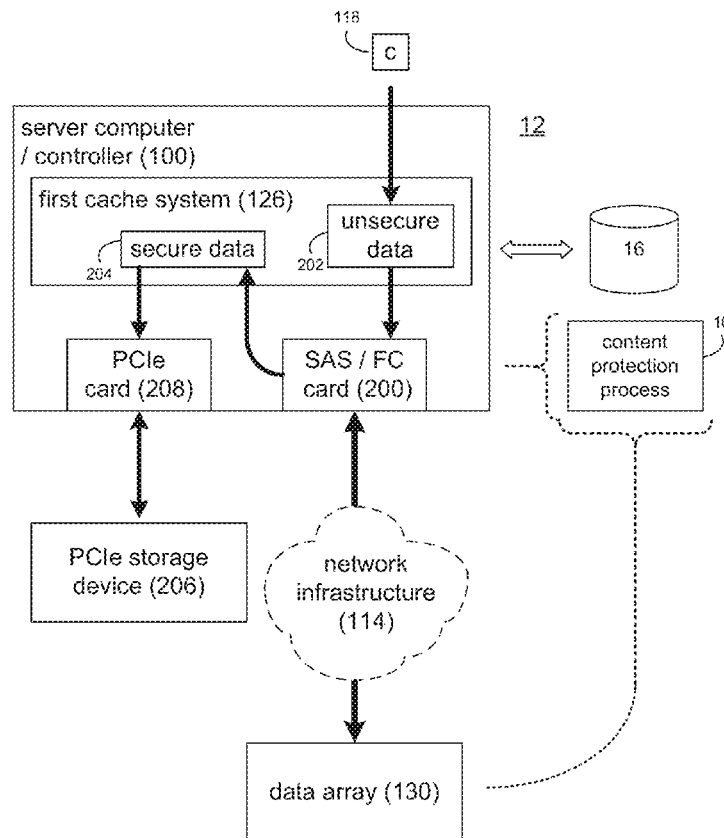
(52) **U.S. Cl.**
CPC **G06F 21/78** (2013.01); **H04L 67/1097** (2013.01); **G06F 2213/0028** (2013.01); **H04L 67/2842** (2013.01); **G06F 3/061** (2013.01)

(58) **Field of Classification Search**
None
See application file for complete search history.

(57) **ABSTRACT**

A method, computer program product, and computing system for receiving an unsecure data portion for storage within a storage system. The unsecure data portion is stored within a temporary storage device. The unsecure data portion is processed to produce a secure data portion via a processor included within a first controller card included within the storage system. The secure data portion is stored on a persistent storage device via a second controller card.

21 Claims, 4 Drawing Sheets



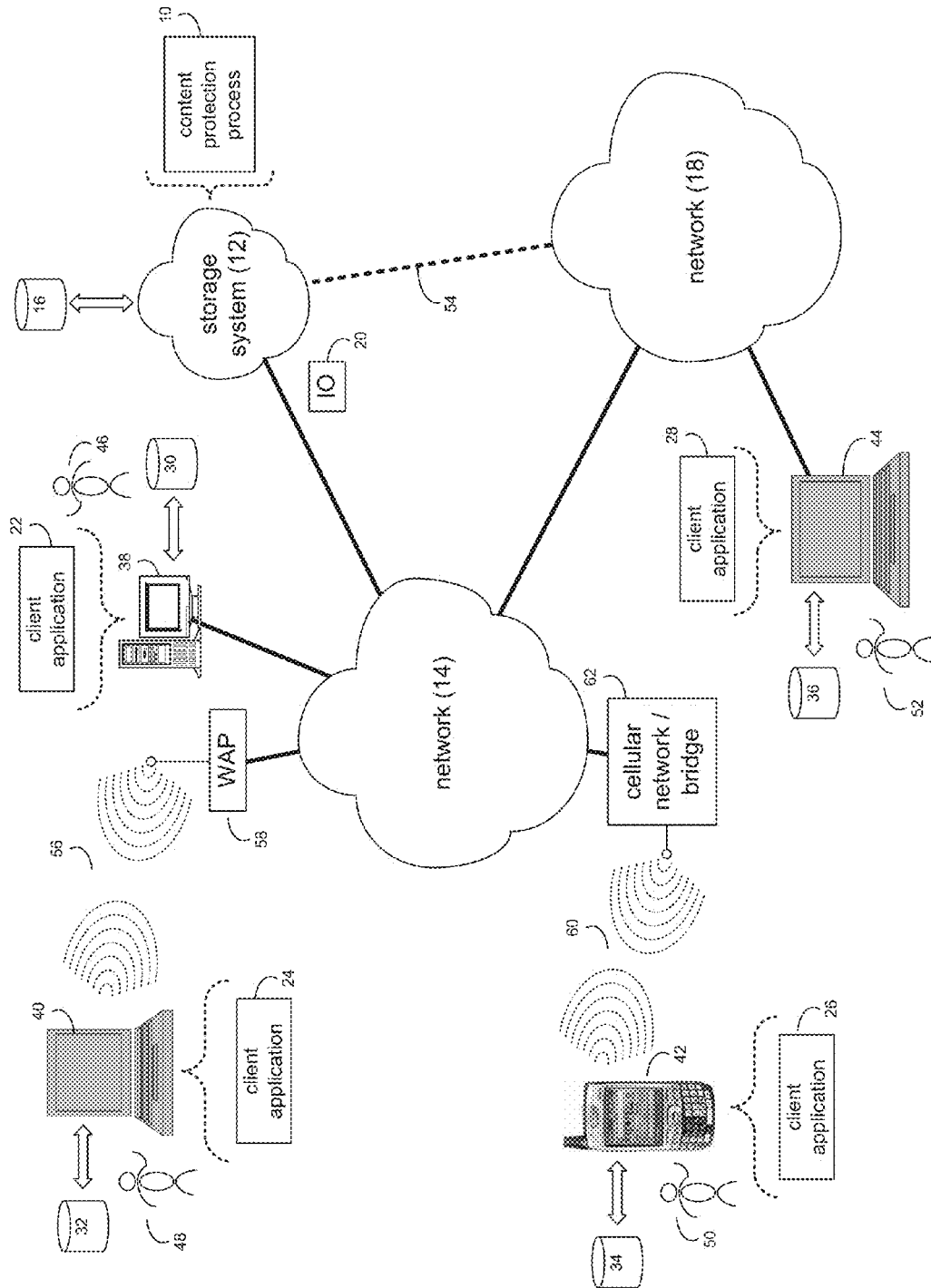


FIG. 1

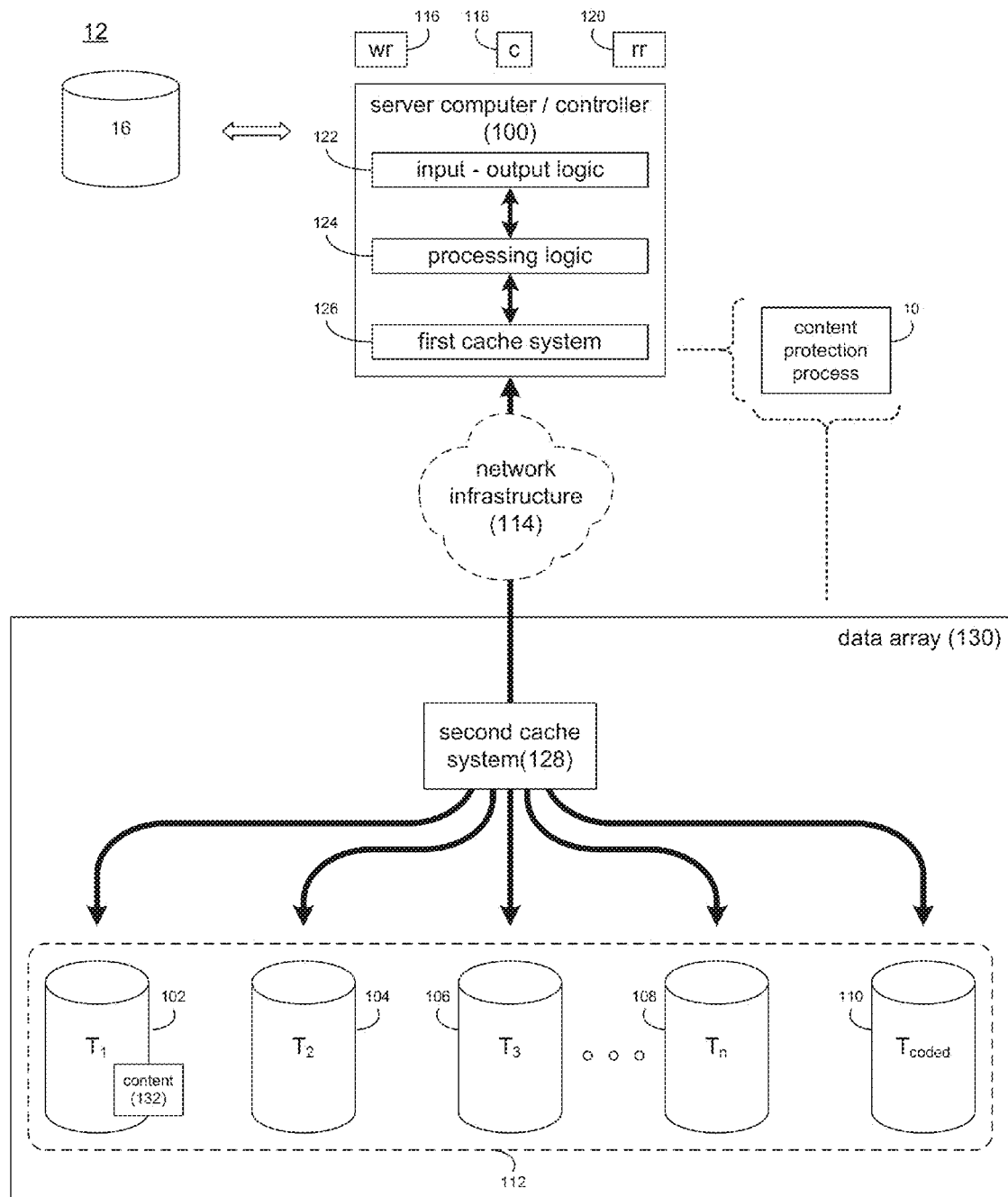


FIG. 2

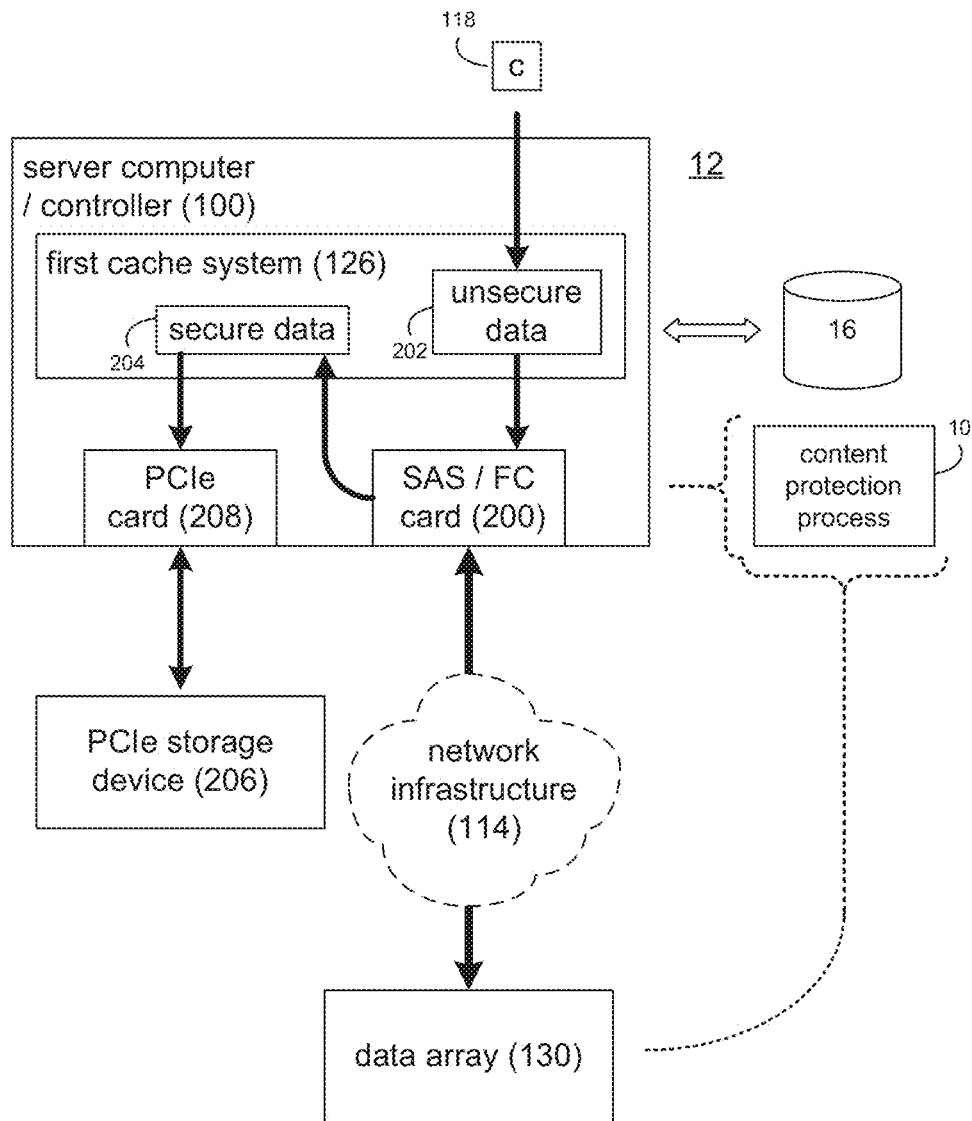


FIG. 3

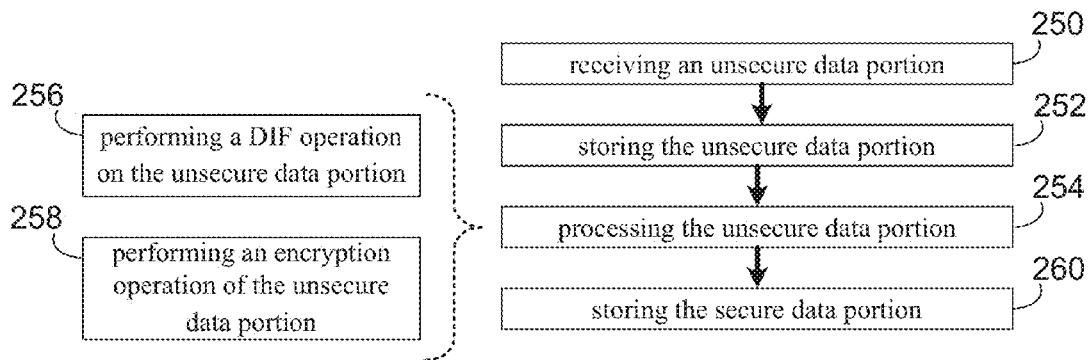
10

FIG. 4

SYSTEM AND METHOD FOR PROTECTING CONTENT

TECHNICAL FIELD

This disclosure relates to electronic content and, more particularly, to systems and methods for protecting electronic content.

BACKGROUND

Storing and safeguarding electronic content is of paramount importance in modern business. Accordingly, various systems may be employed to protect such electronic content.

The use of solid-state storage devices is increasing in popularity. A solid state storage device is a content storage device that uses solid-state memory to store persistent content. A solid-state storage device may emulate (and therefore replace) a conventional hard disk drive. Additionally/alternatively, a solid state storage device may be used within a cache memory system. With no moving parts, a solid-state storage device largely eliminates (or greatly reduces) seek time, latency and other electromechanical delays and failures associated with a conventional hard disk drive.

SUMMARY OF DISCLOSURE

In a first implementation, a computer-implemented method includes receiving an unsecure data portion for storage within a storage system. The unsecure data portion is stored within a temporary storage device. The unsecure data portion is processed to produce a secure data portion via a processor included within a first controller card included within the storage system. The secure data portion is stored on a persistent storage device via a second controller card.

One or more of the following features may be included. The storage system may include a data array. The data array may include a plurality of electromechanical hard disk drives. The persistent storage device may include a flash-based storage device. The first controller card may be chosen from the group consisting of: an SAS controller card that is coupled to one or more SAS storage devices; and a fiber channel controller card that is coupled to one or more fiber channel storage devices. Processing the unsecure data portion to produce a secure data portion may include one or more of: performing a DIF operation on the unsecure data portion; and performing an encryption operation of the unsecure data portion. The temporary storage device may include a cache memory system.

In another implementation, a computer program product resides on a computer readable medium that has a plurality of instructions stored on it. When executed by a processor, the instructions cause the processor to perform operations including receiving an unsecure data portion for storage within a storage system. The unsecure data portion is stored within a temporary storage device. The unsecure data portion is processed to produce a secure data portion via a processor included within a first controller card included within the storage system. The secure data portion is stored on a persistent storage device via a second controller card.

One or more of the following features may be included. The storage system may include a data array. The data array may include a plurality of electromechanical hard disk drives. The persistent storage device may include a flash-based storage device. The first controller card may be chosen from the group consisting of: an SAS controller card that is coupled to one or more SAS storage devices; and a fiber channel con-

troller card that is coupled to one or more fiber channel storage devices. Processing the unsecure data portion to produce a secure data portion may include one or more of: performing a DIF operation on the unsecure data portion; and performing an encryption operation of the unsecure data portion. The temporary storage device may include a cache memory system.

In another implementation, a computing system includes at least one processor and at least one memory architecture coupled with the at least one processor, wherein the computing system is configured to perform operations including receiving an unsecure data portion for storage within a storage system. The unsecure data portion is stored within a temporary storage device. The unsecure data portion is processed to produce a secure data portion via a processor included within a first controller card included within the storage system. The secure data portion is stored on a persistent storage device via a second controller card.

One or more of the following features may be included. The storage system may include a data array. The data array may include a plurality of electromechanical hard disk drives. The persistent storage device may include a flash-based storage device. The first controller card may be chosen from the group consisting of: an SAS controller card that is coupled to one or more SAS storage devices; and a fiber channel controller card that is coupled to one or more fiber channel storage devices. Processing the unsecure data portion to produce a secure data portion may include one or more of: performing a DIF operation on the unsecure data portion; and performing an encryption operation of the unsecure data portion. The temporary storage device may include a cache memory system.

The details of one or more implementations are set forth in the accompanying drawings and the description below. Other features and advantages will become apparent from the description, the drawings, and the claims.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a diagrammatic view of a storage system and a content protection process coupled to a distributed computing network;

FIG. 2 is a diagrammatic view of the storage system of FIG. 1;

FIG. 3 is another diagrammatic view the storage system of FIG. 1.

FIG. 4 is a flow chart of the content protection process of FIG. 1.

Like reference symbols in the various drawings indicate like elements.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

System Overview:

Referring to FIG. 1, there is shown content protection process 10 that may reside on and may be executed by storage system 12, which may be connected to network 14 (e.g., the Internet or a local area network). Examples of storage system 12 may include, but are not limited to: a Network Attached Storage (NAS) system, a Storage Area Network (SAN), a personal computer with a memory system, a server computer with a memory system, and a cloud-based device with a memory system.

As is known in the art, a SAN may include one or more of a personal computer, a server computer, a series of server computers, a mini computer, a mainframe computer, a RAID

device and a NAS system. The various components of storage system 12 may execute one or more operating systems, examples of which may include but are not limited to: Microsoft Windows XP Server™; Novell Netware™; Redhat Linux™ Unix, or a custom operating system, for example.

The instruction sets and subroutines of content protection process 10, which may be stored on storage device 16 included within storage system 12, may be executed by one or more processors (not shown) and one or more memory architectures (not shown) included within storage system 12. Storage device 16 may include but is not limited to: a hard disk drive; a tape drive; an optical drive; a RAID device; a random access memory (RAM); a read-only memory (ROM); and all forms of flash memory storage devices.

Network 14 may be connected to one or more secondary networks (e.g., network 18), examples of which may include but are not limited to: a local area network; a wide area network; or an intranet, for example.

Various IO requests (e.g. IO request 20) may be sent from client applications 22, 24, 26, 28 to storage system 12. Examples of IO request 20 may include but are not limited to IO write requests (i.e. a request that content be written to storage system 12) and IO read requests (i.e. a request that content be read from storage system 12).

The instruction sets and subroutines of client applications 22, 24, 26, 28, which may be stored on storage devices 30, 32, 34, 36 (respectively) coupled to client electronic devices 38, 40, 42, 44 (respectively), may be executed by one or more processors (not shown) and one or more memory architectures (not shown) incorporated into client electronic devices 38, 40, 42, 44 (respectively). Storage devices 30, 32, 34, 36 may include but are not limited to: hard disk drives; tape drives; optical drives; RAID devices; random access memories (RAM); read-only memories (ROM), and all forms of flash memory storage devices. Examples of client electronic devices 38, 40, 42, 44 may include, but are not limited to, personal computer 38, laptop computer 40, personal digital assistant 42, notebook computer 44, a server (not shown), a data-enabled, cellular telephone (not shown), and a dedicated network device (not shown).

Users 46, 48, 50, 52 may access storage system 12 directly through network 14 or through secondary network 18. Further, storage system 12 may be connected to network 14 through secondary network 18, as illustrated with link line 54.

The various client electronic devices may be directly or indirectly coupled to network 14 (or network 18). For example, personal computer 38 is shown directly coupled to network 14 via a hardwired network connection. Further, notebook computer 44 is shown directly coupled to network 18 via a hardwired network connection. Laptop computer 40 is shown wirelessly coupled to network 14 via wireless communication channel 56 established between laptop computer 40 and wireless access point (i.e., WAP) 58, which is shown directly coupled to network 14. WAP 58 may be, for example, an IEEE 802.11a, 802.11b, 802.11g, 802.11n, Wi-Fi, and/or Bluetooth device that is capable of establishing wireless communication channel 56 between laptop computer 40 and WAP 58. Personal digital assistant 42 is shown wirelessly coupled to network 14 via wireless communication channel 60 established between personal digital assistant 42 and cellular network/bridge 62, which is shown directly coupled to network 14.

Client electronic devices 38, 40, 42, 44 may each execute an operating system, examples of which may include but are not limited to Microsoft Windows™, Microsoft Windows CET™, Redhat Linux™, or a custom operating system.

The Data Caching Process:

For the following discussion, client application 22 is going to be described for illustrative purposes. However, this is not intended to be a limitation of this disclosure, as other client applications (e.g., client applications 24, 26, 28) may be equally utilized.

For illustrative purposes, storage system 12 will be described as being a network-based storage system that includes a plurality of electro-mechanical backend storage devices. However, this is for illustrative purposes only and is not intended to be a limitation of this disclosure, as other configurations are possible and are considered to be within the scope of this disclosure. For example and as discussed above, storage system 12 may be a personal computer that includes a single electro-mechanical storage device.

Referring also to FIG. 2, storage system 12 may include a server computer/controller (e.g. server computer/controller 100), and a plurality of storage targets T_{1-n} (e.g. storage targets 102, 104, 106, 108). Storage targets 102, 104, 106, 108 may be configured to provide various levels of performance and/or high availability. For example, one or more of storage targets 102, 104, 106, 108 may be configured as a RAID 0 array, in which data is striped across storage targets. By striping data across a plurality of storage targets, improved performance may be realized. However, RAID 0 arrays do not provide a level of high availability. Accordingly, one or more of storage targets 102, 104, 106, 108 may be configured as a RAID 1 array, in which data is mirrored between storage targets. By mirroring data between storage targets, a level of high availability is achieved as multiple copies of the data are stored within storage system 12.

While storage targets 102, 104, 106, 108 are discussed above as being configured in a RAID 0 or RAID 1 array, this is for illustrative purposes only and is not intended to be a limitation of this disclosure, as other configurations are possible. For example, storage targets 102, 104, 106, 108 may be configured as a RAID 3, RAID 4, RAID 5 or RAID 6 array.

While in this particular example, storage system 12 is shown to include four storage targets (e.g. storage targets 102, 104, 106, 108), this is for illustrative purposes only and is not intended to be a limitation of this disclosure. Specifically, the actual number of storage targets may be increased or decreased depending upon e.g. the level of redundancy/performance/capacity required.

Storage system 12 may also include one or more coded targets 110. As is known in the art, a coded target may be used to store coded data that may allow for the regeneration of data lost/corrupted on one or more of storage targets 102, 104, 106, 108. An example of such a coded target may include but is not limited to a hard disk drive that is used to store parity data within a RAID array.

While in this particular example, storage system 12 is shown to include one coded target (e.g., coded target 110), this is for illustrative purposes only and is not intended to be a limitation of this disclosure. Specifically, the actual number of coded targets may be increased or decreased depending upon e.g. the level of redundancy/performance/capacity required.

Examples of storage targets 102, 104, 106, 108 and coded target 110 may include one or more electro-mechanical hard disk drives, wherein a combination of storage targets 102, 104, 106, 108 and coded target 110 may form non-volatile, electro-mechanical memory system 112.

The manner in which storage system 12 is implemented may vary depending upon e.g. the level of redundancy/performance/capacity required. For example, storage system 12 may be a RAID device in which server computer/controller

100 is a RAID controller card and storage targets 102, 104, 106, 108 and/or coded target 110 are individual “hot-swappable” hard disk drives. An example of such a RAID device may include but is not limited to an NAS device. Alternatively, storage system 12 may be configured as a SAN, in which server computer/controller 100 may be e.g., a server computer and each of storage targets 102, 104, 106, 108 and/or coded target 110 may be a RAID device and/or computer-based hard disk drive. Further still, one or more of storage targets 102, 104, 106, 108 and/or coded target 110 may be a SAN.

In the event that storage system 12 is configured as a SAN, the various components of storage system 12 (e.g. server computer/controller 100, storage targets 102, 104, 106, 108, and coded target 110) may be coupled using network infrastructure 114, examples of which may include but are not limited to an Ethernet (e.g., Layer 2 or Layer 3) network, a fiber channel network, an InfiniBand network, or any other circuit switched/packet switched network.

Storage system 12 may execute all or a portion of content protection process 10. The instruction sets and subroutines of content protection process 10, which may be stored on a storage device (e.g., storage device 16) coupled to server computer/controller 100, may be executed by one or more processors (not shown) and one or more memory architectures (not shown) included within server computer/controller 100. Storage device 16 may include but is not limited to: a hard disk drive; a tape drive; an optical drive; a RAID device; a random access memory (RAM); a read-only memory (ROM); and all forms of flash memory storage devices.

As discussed above, various IO requests (e.g. IO request 20) may be generated. For example, these IO requests may be sent from client applications 22, 24, 26, 28 to storage system 12. Additionally/alternatively and when server computer/controller 100 is configured as an application server, these IO requests may be internally generated within server computer/controller 100. Examples of IO request 20 may include but are not limited to IO write request 116 (i.e. a request that content 118 be written to storage system 12) and IO read request 120 (i.e. a request that content 118 be read from storage system 12).

Server computer/controller 100 may include input-output logic 122 (e.g., a network interface card or a Host Bus Adaptor (HBA)), processing logic 124, and first cache system 126. Examples of first cache system 126 may include but are not limited to a volatile, solid-state, cache memory system (e.g., a dynamic RAM cache memory system) and/or a non-volatile, solid-state, cache memory system (e.g., a flash-based, cache memory system).

During operation of server computer/controller 100, content 118 to be written to storage system 12 may be received by input-output logic 122 (e.g. from network 14 and/or network 18) and processed by processing logic 124. Additionally/alternatively and when server computer/controller 100 is configured as an application server, content 118 to be written to storage system 12 may be internally generated by server computer/controller 100. As will be discussed below in greater detail, processing logic 124 may initially store content 118 within first cache system 126.

Depending on the manner in which first cache system 126 is configured, processing logic 124 may immediately write content 118 to second cache system 128/non-volatile, electro-mechanical memory system 112 (if first cache system 126 is configured as a write-through cache) or may subsequently write content 118 to second cache system 128/non-volatile, electro-mechanical memory system 112 (if first cache system 126 is configured as a write-back cache). Additionally and in

certain configurations, processing logic 124 may calculate and store coded data on coded target 110 (included within non-volatile, electromechanical memory system 112) that may allow for the regeneration of data lost/corrupted on one or more of storage targets 102, 104, 106, 108. For example, if processing logic 124 was included within a RAID controller card or a NAS/SAN controller, processing logic 124 may calculate and store coded data on coded target 110. However, if processing logic 124 was included within e.g., an applications server, data array 130 may calculate and store coded data on coded target 110.

Examples of second cache system 128 may include but are not limited to a volatile, solid-state, cache memory system (e.g., a dynamic RAM cache memory system) and/or a non-volatile, solid-state, cache memory system (e.g., a flash-based, cache memory system).

The combination of second cache system 128 and non-volatile, electromechanical memory system 112 may form data array 130, wherein first cache system 126 may be sized so that the number of times that data array 130 is accessed may be reduced. Accordingly, by sizing first cache system 126 so that first cache system 126 retains a quantity of data sufficient to satisfy a significant quantity of IO requests (e.g., IO request 20), the overall performance of storage system 12 may be enhanced. As will be described below in greater detail, first cache system 126 may be a content-aware cache system.

Further, second cache system 128 within data array 130 may be sized so that the number of times that non-volatile, electromechanical memory system 112 is accessed may be reduced. Accordingly, by sizing second cache system 128 so that second cache system 128 retains a quantity of data sufficient to satisfy a significant quantity of IO requests (e.g., IO request 20), the overall performance of storage system 12 may be enhanced.

As discussed above, the instruction sets and subroutines of content protection process 10, which may be stored on storage device 16 included within storage system 12, may be executed by one or more processors (not shown) and one or more memory architectures (not shown) included within storage system 12. Accordingly, in addition to being executed on server computer/controller 100, some or all of the instruction sets and subroutines of content protection process 10 may be executed by one or more processors (not shown) and one or more memory architectures (not shown) included within data array 130.

The Content Protection Process:

Referring also to FIG. 3, there is shown a manner in which storage system 12 may be configured to secure content stored within storage system 12. Specifically, assume for illustrative purposes that data array 130 may include SAS disk drives and/or fiber channel disk drives. Accordingly, controller card 200 may include: an SAS controller card and/or a fiber channel controller card. Therefore, if any of the electro-mechanical hard disk drives included within data array 130 are SAS disk drives, controller card 200 may be an SAS controller card. Further, if any of the electro-mechanical hard disk drives included within data array 130 are fiber channel disk drives, controller card 200 may be a fiber channel controller card. In the event that both SAS and fiber channel disk drives are included within data array 130, controller card 200 may actually include two separate controller cards, namely one SAS controller card and one fiber channel controller card.

Assume for illustrative purposes that IO write request 116 (i.e. a request that content 118 be written to storage system 12) is being processed by storage system 12. Content protection process 10 may receive 250 content 118 for storage

within storage system **12**, which may be stored **252** (as unsecure data portion **202**) at a first memory address within a temporary storage device (e.g., first cache system **126**).

Once stored within first cache system **126**, content protection process **10** may notify first controller card (e.g., controller card **200**) that unsecure data portion **202** is stored at the first memory address within the temporary storage device (e.g., first cache system **126**). Content protection process **10** may then process **254** unsecure data portion **202** to produce secure data portion **204** via a processor (not shown) included within first controller card **200** included within storage system **12**.

When processing **254** unsecure data portion **202** to produce secure data portion **204**, content protection process **10** may perform one of a plurality of procedures (via a processor (not shown) included within first controller card **200**). For example, content protection process **10** may perform **256** a DIF operation (i.e., adding a data integrity field) on unsecure data portion **202**; and may perform **258** an encryption operation of unsecure data portion **202**.

Concerning the DIF operation performed **256** by content protection process **10**, fiber channel and SAS protocols typically communicate using 512 byte data blocks, typically sixteen blocks at a time (to make an 8 kb sector). When performing **256** a DIF operation on such a 512 byte block, content protection process **10** may add an eight byte DIF field (not shown) to each 512 byte data block. Concerning the structure of this eight byte DIF field, two bytes may be reserved for a CRC (i.e., a Cyclic Redundancy Check), four bytes may be reserved for a Ref Tag (i.e., an incrementing value that defines the sequence for assembling the sector from the individual 512 byte data blocks), and two bytes may be reserved for an App Tag (i.e., an identifier that identifies that application that is associated with the sector).

As is known in the art, CRC is an error-detecting code commonly used in digital networks and storage devices to detect data corruption. Blocks of data entering such networks/devices typically get a short check value attached to the data blocks, wherein the value is based upon the remainder of a polynomial division of the content of the data block. Upon retrieval of the data block, the calculation is repeated to see if it matches the initial calculation. If it does not, data corruption exists.

Concerning the encryption operation performed **258** to produce secure data portion **204**, content protection process **10** may perform a standard AES type encryption procedure on unsecure data portion **202**. As is known in the art, AES is a specification for the encryption of electronic data, which has been adopted by the U.S. government and is now widely used. The algorithm described by AES is a symmetric-key algorithm, wherein the same key is used for both encrypting and decrypting the data.

When the processing **254** of unsecure data portion **202** is complete, content protection process **10** may store secure data portion **204** at a second memory address within a temporary storage device (e.g., first cache system **126**), without first storing secure data portion **204** on data array **130** (as controller card **200** is configured to loop secure data portion **204** back to first cache system **126**). Content protection process **10** may store **260** secure data portion **204** on persistent storage device (e.g., flash-based PCIe storage device **206**) via second controller card **208** (e.g., a PCIe controller card).

General:

As will be appreciated by one skilled in the art, the present disclosure may be embodied as a method, a system, or a computer program product. Accordingly, the present disclosure may take the form of an entirely hardware embodiment,

an entirely software embodiment (including firmware, resident software, micro-code, etc.) or an embodiment combining software and hardware aspects that may all generally be referred to herein as a "circuit," "module" or "system." Furthermore, the present disclosure may take the form of a computer program product on a computer-usable storage medium having computer-usable program code embodied in the medium.

Any suitable computer usable or computer readable medium may be utilized. The computer-usable or computer-readable medium may be, for example but not limited to, an electronic, magnetic, optical, electromagnetic, infrared, or semiconductor system, apparatus, device, or propagation medium. More specific examples (a non-exhaustive list) of the computer-readable medium may include the following: an electrical connection having one or more wires, a portable computer diskette, a hard disk, a random access memory (RAM), a read-only memory (ROM), an erasable programmable read-only memory (EPROM or Flash memory), an optical fiber, a portable compact disc read-only memory (CD-ROM), an optical storage device, a transmission media such as those supporting the Internet or an intranet, or a magnetic storage device. The computer-usable or computer-readable medium may also be paper or another suitable medium upon which the program is printed, as the program can be electronically captured, via, for instance, optical scanning of the paper or other medium, then compiled, interpreted, or otherwise processed in a suitable manner, if necessary, and then stored in a computer memory. In the context of this document, a computer-usable or computer-readable medium may be any medium that can contain, store, communicate, propagate, or transport the program for use by or in connection with the instruction execution system, apparatus, or device. The computer-usable medium may include a propagated data signal with the computer-usable program code embodied therewith, either in baseband or as part of a carrier wave. The computer usable program code may be transmitted using any appropriate medium, including but not limited to the Internet, wireline, optical fiber cable, RF, etc.

Computer program code for carrying out operations of the present disclosure may be written in an object oriented programming language such as Java, Smalltalk, C++ or the like. However, the computer program code for carrying out operations of the present disclosure may also be written in conventional procedural programming languages, such as the "C" programming language or similar programming languages. The program code may execute entirely on the user's computer, partly on the user's computer, as a stand-alone software package, partly on the user's computer and partly on a remote computer or entirely on the remote computer or server. In the latter scenario, the remote computer may be connected to the user's computer through a local area network/a wide area network/the Internet (e.g., network **14**).

The present disclosure is described with reference to flowchart illustrations and/or block diagrams of methods, apparatus (systems) and computer program products according to embodiments of the disclosure. It will be understood that each block of the flowchart illustrations and/or block diagrams, and combinations of blocks in the flowchart illustrations and/or block diagrams, may be implemented by computer program instructions. These computer program instructions may be provided to a processor of a general purpose computer/special purpose computer/other programmable data processing apparatus, such that the instructions, which execute via the processor of the computer or other programmable data

processing apparatus, create means for implementing the functions/acts specified in the flowchart and/or block diagram block or blocks.

These computer program instructions may also be stored in a computer-readable memory that may direct a computer or other programmable data processing apparatus to function in a particular manner, such that the instructions stored in the computer-readable memory produce an article of manufacture including instruction means which implement the function/act specified in the flowchart and/or block diagram block or blocks.

The computer program instructions may also be loaded onto a computer or other programmable data processing apparatus to cause a series of operational steps to be performed on the computer or other programmable apparatus to produce a computer implemented process such that the instructions which execute on the computer or other programmable apparatus provide steps for implementing the functions/acts specified in the flowchart and/or block diagram block or blocks.

The flowcharts and block diagrams in the figures may illustrate the architecture, functionality, and operation of possible implementations of systems, methods and computer program products according to various embodiments of the present disclosure. In this regard, each block in the flowchart or block diagrams may represent a module, segment, or portion of code, which comprises one or more executable instructions for implementing the specified logical function(s). It should also be noted that, in some alternative implementations, the functions noted in the block may occur out of the order noted in the figures. For example, two blocks shown in succession may, in fact, be executed substantially concurrently, or the blocks may sometimes be executed in the reverse order, depending upon the functionality involved. It will also be noted that each block of the block diagrams and/or flowchart illustrations, and combinations of blocks in the block diagrams and/or flowchart illustrations, may be implemented by special purpose hardware-based systems that perform the specified functions or acts, or combinations of special purpose hardware and computer instructions.

The terminology used herein is for the purpose of describing particular embodiments only and is not intended to be limiting of the disclosure. As used herein, the singular forms “a”, “an” and “the” are intended to include the plural forms as well, unless the context clearly indicates otherwise. It will be further understood that the terms “comprises” and/or “comprising,” when used in this specification, specify the presence of stated features, integers, steps, operations, elements, and/or components, but do not preclude the presence or addition of one or more other features, integers, steps, operations, elements, components, and/or groups thereof.

The corresponding structures, materials, acts, and equivalents of all means or step plus function elements in the claims below are intended to include any structure, material, or act for performing the function in combination with other claimed elements as specifically claimed. The description of the present disclosure has been presented for purposes of illustration and description, but is not intended to be exhaustive or limited to the disclosure in the form disclosed. Many modifications and variations will be apparent to those of ordinary skill in the art without departing from the scope and spirit of the disclosure. The embodiment was chosen and described in order to best explain the principles of the disclosure and the practical application, and to enable others of ordinary skill in the art to understand the disclosure for various embodiments with various modifications as are suited to the particular use contemplated.

A number of implementations have been described. Having thus described the disclosure of the present application in detail and by reference to embodiments thereof, it will be apparent that modifications and variations are possible without departing from the scope of the disclosure defined in the appended claims.

What is claimed is:

1. A computer-implemented method comprising:
 - receiving an unsecure data portion for storage within a storage system;
 - storing the unsecure data portion within a first memory address within a temporary storage device wherein the temporary storage device is a memory device;
 - processing the unsecure data portion to produce a secure data portion via a processor included within a first controller card included within the storage system, wherein the first controller card includes a serial attached small computer system interface (“SAS”) controller card that is coupled to one or more SAS storage devices;
 - storing the secure data portion within a second memory address within the temporary storage device; and
 - storing the secure data portion on a persistent storage device via a second controller card.
2. The computer-implemented method of claim 1 wherein the storage system includes a data array.
3. The computer-implemented method of claim 2 wherein the data array includes a plurality of electromechanical hard disk drives.
4. The computer-implemented method of claim 1 wherein the persistent storage device includes a flash-based storage device.
5. The computer-implemented method of claim 1 wherein the second controller card includes a fiber channel controller card that is coupled to one or more fiber channel storage devices.
6. The computer-implemented method of claim 1 wherein processing the unsecure data portion to produce a secure data portion includes one or more of:
 - performing a data integrity field (“DIF”) operation on the unsecure data portion; and
 - performing an encryption operation of the unsecure data portion.
7. The computer-implemented method of claim 1 wherein the temporary storage device includes a cache memory system.
8. A computer program product residing on a non-transitory computer readable medium having a plurality of instructions stored thereon which, when executed by a processor, cause the processor to perform operations comprising:
 - receiving an unsecure data portion for storage within a storage system;
 - storing the unsecure data portion within a first memory address within a temporary storage device wherein the temporary storage device is a memory device;
 - processing the unsecure data portion to produce a secure data portion via a processor included within a first controller card included within the storage system, wherein the first controller card includes a serial attached small computer system interface (“SAS”) controller card that is coupled to one or more SAS storage devices;
 - storing the secure data portion within a second memory address within the temporary storage device; and
 - storing the secure data portion on a persistent storage device via a second controller card.
9. The computer program product of claim 8 wherein the storage system includes a data array.

11

10. The computer program product of claim 9 wherein the data array includes a plurality of electromechanical hard disk drives.

11. The computer program product of claim 8 wherein the persistent storage device includes a flash-based storage device. 5

12. The computer program product of claim 8 wherein the second controller card includes a fiber channel controller card that is coupled to one or more fiber channel storage devices.

13. The computer program product of claim 8 wherein the instructions for processing the unsecure data portion to produce a secure data portion include instructions for one or more of: 10

performing a data integrity field ("DIF") operation on the unsecure data portion; and

performing an encryption operation of the unsecure data portion. 15

14. The computer program product of claim 8 wherein the temporary storage device includes a cache memory system.

15. A computing system including at least one processor and at least one memory architecture coupled with the at least one processor, wherein the computing system is configured to perform operations comprising: 20

receiving an unsecure data portion for storage within a storage system;

storing the unsecure data portion within a first memory address within a temporary storage device wherein the temporary storage device is a memory device; 25

processing the unsecure data portion to produce a secure data portion via a processor included within a first con-

12

troller card included within the storage system, wherein the first controller card includes a serial attached small computer system interface ("SAS") controller card that is coupled to one or more SAS storage devices;

storing the secure data portion within a second memory address within the temporary storage device; and storing the secure data portion on a persistent storage device via a second controller card.

16. The computing system of claim 15 wherein the storage system includes a data array. 10

17. The computing system of claim 16 wherein the data array includes a plurality of electromechanical hard disk drives.

18. The computing system of claim 15 wherein the persistent storage device includes a flash-based storage device. 15

19. The computing system of claim 15 wherein the second controller card includes a fiber channel controller card that is coupled to one or more fiber channel storage devices.

20. The computing system of claim 15 wherein processing the unsecure data portion to produce a secure data portion includes one or more of: 20

performing a data integrity field ("DIF") operation on the unsecure data portion; and

performing an encryption operation of the unsecure data portion. 25

21. The computing system of claim 15 wherein the temporary storage device includes a cache memory system.

* * * * *